

REMARKS

In the Official Action mailed on **July 14, 2004**, the Examiner reviewed claims 1-33. Claims 1, 12, and 23 were rejected under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement. Claims 1-33 were rejected under 35 U.S.C. §102(e) as being anticipated by Boneh et al (USPN 6,134,660, hereinafter “Boneh”).

Rejections under 35 U.S.C. §112, first paragraph

Claims 1, 12, and 23 were rejected as failing to comply with the written description requirement.

Applicant has amended independent claims 1, 12, and 23 to clarify that the set of information is not available to a user from the system. These amendments find support on page 10, lines 10-14 of the instant application.

Rejections under 35 U.S.C. §102(e)

Claims 1-33 were rejected as being anticipated by Boneh. Applicant respectfully points out that Boneh teaches enabling a user to **manipulate the key file** as desired (see Boneh, col. 10, lines 19-20).

In contrast, the present invention (1) sends information in encrypted form to an information sink, (2) sends the key (or keys) to the information sink, and (3) includes sufficient logic to prevent an information sink (user) from **persistently storing a key or keys** received from the key manager for decrypting the encrypted form of the data (see page 14, lines 9-12 of the instant application). This is beneficial because if neither the decrypted information nor the key is persistently stored at the information sink, the key must be resent to the information sink to decrypt the information again. This helps in restricting access to the information at the sink (please see page 13, line 16 to page 14, line 15 of the instant application). There is nothing within Boneh, either explicit or implicit, which

suggests including sufficient logic to prevent an information sink from persistently storing a key or keys received from the key manager for decrypting the encrypted form of the data.

Accordingly, Applicant has amended independent claims 1, 12, and 23 to include the limitations from dependent claims 7, 18, and 29, respectively, and to clarify that the present invention includes sufficient logic to prevent an information sink from persistently storing a key or keys received from the key manager for decrypting the encrypted form of the data. These amendments find support in original claims 7, 18, and 29 and on page 14, lines 9-12 of the instant application. Dependent claims 7, 18, and 29 have been canceled without prejudice. Dependent claims 8, 19, and 30 have been amended to correct antecedent basis.

Hence, Applicant respectfully submits that independent claims 1, 12, and 23 as presently amended are in condition for allowance. Applicant also submits that claims 2-6 and 8-11, which depend upon claim 1, claims 13-17 and 19-22, which depend upon claim 12, and claims 24-28 and 30-33, which depend upon claim 23, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By


Edward J. Grundler
Registration No. 47, 615

Date: October 6, 2004

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
508 Second Street, Suite 201
Davis, CA 95616-4692
Tel: (530) 759-1663
FAX: (530) 759-1665